PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-014441

(43)Date of publication of application : 19.01.2001

(51)Int.Cl. G06K 19/073
G06F 12/14
G06K 17/00
H04L 9/32

(21)Application number : 11-374788

(22)Date of filing : 28.12.1999

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(72)Inventor : HIROTA TERUTO
TATEBAYASHI MAKOTO
YUGAWA YASUHEI
MINAMI MASANAO
KOZUKA MASAYUKI

(30)Priority

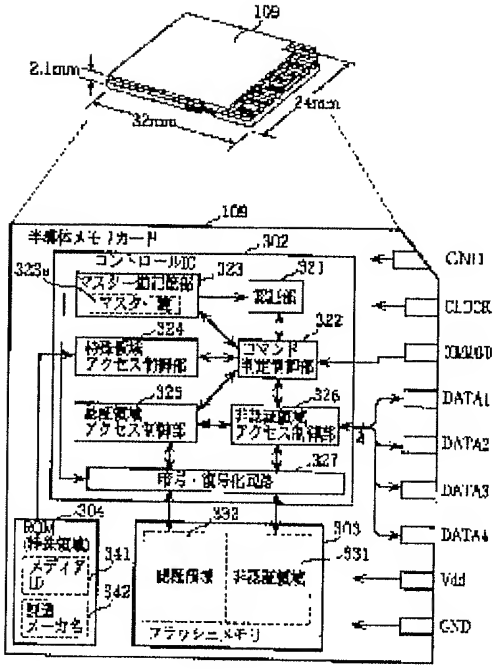
Priority number : 11119441 Priority date : 27.04.1999 Priority country : JP

(54) SEMICONDUCTOR MEMORY CARD AND READER

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a semiconductor memory card usable as a storage medium for digital literary works and also usable as a storage medium for general computer data (non-literary works) for which the protection of copyright is not required.

SOLUTION: This card is composed of a control IC 302, a flash memory 303 and a ROM 304, the ROM 304 holds a medium ID 341 or the like peculiar to this card, the flash memory 303 has an authentication area 332 for permitting access to external equipment only when the authentication of that external equipment is made successful and a non-authentication area 331 for permitting access regardless of the authenticated result and the control IC 302 has control parts 325 and 326 for controlling access from the external equipment to the authentication area 332 and the non-authentication area 331 and an authentication part 321 or the like for executing mutual authentication with the external equipment.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－14441
(P2001－14441A)
(43)公開日　平成13年１月19日(2001.1.19)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード（参考）
Ｇ０６Ｋ　19/073		Ｇ０６Ｋ　19/00	Ｐ　５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ａ　５Ｂ０３５
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｅ　５Ｂ０５８
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ａ　５Ｊ１０４
			６７５Ｄ

審査請求　未請求　請求項の数17　ＯＬ　（全 27 頁）

(21)出願番号　特願平11－374788

(22)出願日　平成11年12月28日(1999.12.28)

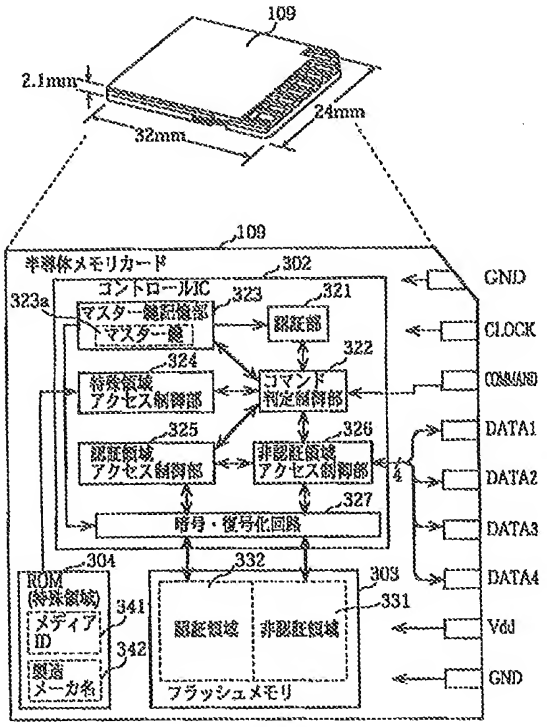
(31)優先権主張番号　特願平11－119441
(32)優先日　平成11年４月27日(1999.4.27)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　廣田　照人
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　館林　誠
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100090446
弁理士　中島　司朗　（外１名）

最終頁に続く

(54)【発明の名称】　半導体メモリカード及び読み出し装置

(57)【要約】
【課題】　デジタル著作物の記憶媒体として用いることが可能であり、かつ、著作権保護が必要とされない一般的なコンピュータデータ（非著作物）の記憶媒体としても用いることが可能な半導体メモリカードを提供する。
【解決手段】　コントロールＩＣ３０２とフラッシュメモリ３０３とＲＯＭ３０４とからなり、ＲＯＭ３０４は、このカードに固有のメディアＩＤ３４１等を保持し、フラッシュメモリ３０３は、外部機器の認証に成功した場合にのみその外部機器にアクセスを許可する認証領域３３２と認証の結果に拘わらずアクセスを許可する非認証領域３３１とを有し、コントロールＩＣ３０２は、外部機器による認証領域３３２及び非認証領域３３１へのアクセスを制御する制御部３２５、３２６及び外部機器との相互認証を実行する認証部３２１等を有する。



と物理アドレスとの対応を示す変換テーブルと、
前記電子機器からの命令に従って前記変換テーブルを変更する変換テーブル変更部とを有し、
前記認証領域アクセス制御部及び前記非認証領域アクセス制御部は、前記変換テーブルに基づいて前記電子機器によるアクセスを制御することを特徴とする請求項１記載の半導体メモリカード。
【請求項１３】　前記制御回路はさらに、前記認証領域及び前記非認証領域に書き込むべきデータを暗号化するとともに、前記認証領域及び前記非認証領域から読み出されたデータを復号化する暗号復号部を有することを特徴とする請求項１記載の半導体メモリカード。
【請求項１４】　前記不揮発メモリは、フラッシュメモリであり、
前記制御回路はさらに、前記電子機器からの命令に従って、前記認証領域及び前記認証領域に存在する未消去の領域を特定し、その領域を示す情報を前記電子機器に送る未消去リスト読み出し部を有することを特徴とする請求項１記載の半導体メモリカード。
【請求項１５】　前記認証部は、認証のために電子機器を使用するユーザに対してそのユーザに固有の情報であるユーザキーを要求するものであり、
前記制御回路はさらに、
前記ユーザキーを記憶しておくためのユーザキー記憶部と、
前記認証部による認証に成功した電子機器を特定することができる識別情報を記憶しておくための識別情報記憶部と、
前記認証部による認証が開始されると、その電子機器から識別情報を取得し、その識別情報が前記識別情報記憶部に既に格納されているか否か検査し、既に格納されている場合には、前記認証部によるユーザキーの要求を禁止させるユーザキー要求禁止部とを有することを特徴とする請求項１記載の半導体メモリカード。
【請求項１６】　請求項１記載の半導体メモリカードに格納されたデジタル著作物を読み出す読み出し装置であって、
前記半導体メモリカードは、非認証領域に、デジタル著作物が格納されているとともに、認証領域に、前記デジタル著作物の読み出しを許可する回数が予め格納され、
前記読み出し装置は、
前記非認証領域に格納されたデジタル著作物を読み出す際に、前記認証領域に格納された回数を読み出し、その回数によって読み出しが許可されているか否か判断する判断手段と、
許可されている場合にのみ前記非認証領域から前記デジタル著作物を読み出すとともに、読み出した前記回数を減算して前記認証領域に書き戻す再生手段とを備えることを特徴とする読み出し装置。
【請求項１７】　請求項１記載の半導体メモリカードに格納されたデジタル著作物を読み出してアナログ信号に再生する読み出し装置であって、
前記半導体メモリカードは、非認証領域に、アナログ信号に再生可能なデジタル著作物が格納されているとともに、認証領域に、前記デジタル著作物の前記電子機器によるデジタル出力を許可する回数が予め格納され、
前記読み出し装置、
前記非認証領域に格納されたデジタル著作物を読み出してアナログ信号に再生する再生手段と、
前記認証領域に格納された回数を読み出し、その回数によってデジタル出力が許可されているか否か判断する判断手段と、
許可されている場合にのみ前記デジタル著作物をデジタル信号のまま外部に出力するとともに、読み出した前記回数を減算して前記認証領域に書き戻すデジタル出力手段とを備えることを特徴とする読み出し装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、デジタル著作物等を記憶するための半導体メモリカード及びその読み出し装置に関し、特に、デジタル著作物の著作権保護に好適な半導体メモリカード及び読み出し装置に関する。
【０００２】
【従来の技術】近年、マルチメディア・ネットワーク技術の発展により、音楽コンテンツ等のデジタル著作物がインターネット等の通信ネットワークを通じて配信されるようになり、自宅に居ながらにして世界中の音楽等に接することが可能となってきた。例えば、パーソナルコンピュータ（以下、「ＰＣ」という。）で音楽コンテンツをダウンロードした後、ＰＣに装着された半導体メモリカードに格納しておくことで、必要に応じて音楽を再生し楽しむことができる。また、このようにして音楽コンテンツを格納した半導体メモリカードをＰＣから取り出して携帯型音楽再生装置に装着しておくことで、歩きながら音楽を聴くこともできる。このような半導体メモリカードは、フラッシュメモリ等の不揮発性で、かつ、大きな記憶容量の半導体メモリを内蔵した小型軽量の便利なカードである。
【０００３】ところで、このような電子音楽配信において、半導体メモリカードにデジタル著作物を記憶する場合、不正なコピーを防止するために、鍵等を用いてコンテンツを暗号化しておく必要がある。また、ＰＣ等に標準添付されて広く出回っているファイル管理ソフトウェアによっては他の記憶媒体等にコピーすることができないようにしておく必要もある。
【０００４】このような不正なコピーを防止する方法として、半導体メモリカードへのアクセスを専用のソフトウェアでのみ可能とする方策が考えられる。例えば、ＰＣと半導体メモリカード間での認証が成功した時にのみ半導体メモリカードへのアクセスを許可することとし、

き込みが許可されている場合には、そのアプリケーションは、暗号化された音楽データ、パスワード、権利情報をメモリカード１０９に書き込むことができる。図２は、このメモリカード１０９を記録媒体とする携帯型の録音再生装置（以下、「プレーヤ」という。）２０１の外観を示す図である。

【００１５】プレーヤ２０１の上面には、液晶表示部２０３と操作ボタン２０２が設けられ、手前側面には、メモリカード１０９を着脱するためのメモリカード挿入口２０６及びＰＣ１０２等と接続するためのＵＳＢ等の通信ポート２１３が設けられ、右側面には、アナログ出力端子２０４、デジタル出力端子２０５及びアナログ入力端子２２３等が設けられている。

【００１６】プレーヤ２０１は、メモリカード１０９に格納された音楽データ、パスワード、権利情報に基づいて、再生が許可されている状態にあるならば、その音楽データを読み出して復号した後にアナログ信号に変換し、アナログ出力端子２０４に接続されたヘッドフォン２０８を通じて音声として出力したり、再生中の音楽データをデジタルデータのままデジタル出力端子２０５に出力したりする。

【００１７】また、このプレーヤ２０１は、マイク等を介してアナログ入力端子２２３から入力されるアナログの音声信号をデジタルデータに変換してメモリカード１０９に記録したり、通信ポート２１３を介して接続されたＰＣ１０２と通信することによって、そのＰＣ１０２によってダウンロードされた音楽データ、パスワード及び権利情報をメモリカード１０９に記録することができる。つまり、このプレーヤ２０１は、メモリカード１０９への音楽データの記録及びメモリカード１０９に記録された音楽データの再生に関して、図１に示されたＰＣ１０２及びメモリカードライタ１０７に置き換わる機能を有する。

【００１８】図３は、ＰＣ１０２のハードウェア構成を示すブロック図である。ＰＣ１０２は、ＣＰＵ１１０、デバイス鍵１１１ａや制御プログラム１１１ｂ等を予め記憶しているＲＯＭ１１１、ＲＡＭ１１２、ディスプレイ１０３、通信回線１０１と接続するためのモデムポートやプレーヤ２０１と接続するためのＵＳＢ等を備える通信ポート１１３、キーボード１０４、内部バス１１４、メモリカード１０９と内部バス２１４とを接続するメモリカードライタ１０７、メモリカード１０９から読み出された暗号化音楽データを復号するデスクランブラ１１１７、復号された音楽データを伸張するＭＰＥＧ２－ＡＡＣ（ＩＳＯ１３８１８－７）に準拠したＡＡＣデコーダ１１８、伸張されたデジタル音楽データをアナログ音声信号に変換するＤ／Ａコンバータ１１９、スピーカ１０６及びファイル管理ソフトウェアやアプリケーションを格納しているハードディスク１２０等から構成される。

【００１９】このＰＣ１０２は、ハードディスク１２０に格納されたファイル管理ソフトウェアを実行することで、メモリカード１０９をハードディスクのように独立したファイルシステム（ＩＳＯ９２９３等）を有する補助記憶装置として用いることができるだけでなく、ハードディスク１２０に格納された上述の専用アプリケーションを実行することで、通信ポート１１３のモデム等を介して通信回線１０１から音楽コンテンツ等をダウンロードしたり、メモリカード１０９との相互認証を行なった後に音楽コンテンツ等をメモリカード１０９に格納したり、メモリカード１０９に格納されている音楽コンテンツ等を読み出してスピーカ１０６に再生出力したりする。

【００２０】なお、ＲＯＭ１１１に格納されたデバイス鍵１１１ａは、このＰＣ１０２に固有の秘密鍵であり、後述するように、相互認証等に用いられる。図４は、プレーヤ２０１のハードウェア構成を示すブロック図である。プレーヤ２０１は、ＣＰＵ２１０、デバイス鍵２１１ａや制御プログラム２１１ｂ等を予め記憶しているＲＯＭ２１１、ＲＡＭ２１２、液晶表示部２０３、ＰＣ１０２等と接続するためのＵＳＢ等の通信ポート２１３、操作ボタン２０２、内部バス２１４、メモリカード１０９と内部バス２１４とを接続するカードＩ／Ｆ部２１５、メモリカード１０９との相互認証を実行する認証回路２１６、メモリカード１０９から読み出された暗号化音楽データを復号するデスクランブラ２１７、復号された音楽データ伸張するＭＰＥＧ２－ＡＡＣ（ＩＳＯ１３８１８－７）に準拠したＡＡＣデコーダ２１８、伸張されたデジタル音楽データをアナログ音声信号に変換するＤ／Ａコンバータ２１９、スピーカ２２４、アナログ入力端子２２３から入力されたアナログ音楽信号をデジタル音楽データに変換をするＡ／Ｄコンバータ２２１、そのデジタル音楽データをＭＰＥＧ２－ＡＡＣ（ＩＳＯ１３８１８－７）に準拠して圧縮符号化するＡＡＣエンコーダ２２０、圧縮符号化された音楽データを暗号化するスクランブラ２２２、アナログ出力端子２０４、デジタル出力端子２０５及びアナログ入力端子２２３から構成される。

【００２１】このプレーヤ２０１は、ＲＯＭ２１１に格納された制御プログラム２１１ｂをＲＡＭ２１２にロードしＣＰＵ２１０に実行させることで、メモリカード１０９に格納されている音楽コンテンツ等を読み出してスピーカ２２４に再生出力したり、アナログ入力端子２２３や通信ポート２１３を経て入力された音楽コンテンツ等をメモリカード１０９に格納したりする。つまり、通常のプレーヤと同様に、個人的に音楽を録音したり再生したりして楽しむことができるだけでなく、ＰＣ１０２によりダウンロードされた電子音楽配信に係る（著作権保護が必要とされる）音楽コンテンツの記録・再生もできる。

む際にそのデータを暗号化して書き込み、フラッシュメモリ３０３からデータを読み出した際にそのデータを復号化する。これは、不正なユーザがこのメモリカード１０９を分解してフラッシュメモリ３０３の内容を直接解析し、認証領域３３２に格納されたパスワードを盗む等の不正行為を防止するためである。

【００３１】なお、コントロールＩＣ３０２は、これら主要な構成要素３２１～３２７の他に、クロックピンから供給されるクロック信号に同期した内部クロック信号を生成し各構成要素に供給する同期回路や、揮発性の記憶領域及び不揮発性の記憶領域等を有する。また、特殊領域（ＲＯＭ３０４）に格納されている情報の改ざんを防止するために、そのＲＯＭ３０４をコントロールＩＣ３０２の中に内蔵させたり、それらの情報をフラッシュメモリ３０３に格納し、外部から書き込みできないように特殊領域アクセス制御部３２４が制限をかけてもよい。そのときに、暗号・復号化回路３２７で暗号化したデータを格納することとしてもよい。

【００３２】図６は、ＰＣ１０２やプレーヤ２０１から見たメモリカード１０９の記憶領域の種類を示す図である。メモリカード１０９が有する記憶領域は、大きく分けて、特殊領域３０４と認証領域３３２と非認証領域３３１の３つの領域である。特殊領域３０４は読み出し専用の領域で、この中のデータに対しては、専用コマンドを用いて読み出しを行う。認証領域３３２は、ＰＣ１０２又はプレーヤ２０１とメモリカード１０９との間で認証が成功した時にのみ読み書きができる領域で、この領域へのアクセスについては暗号化されたコマンドを用いる。非認証領域３３１は、ＡＴＡやＳＣＳＩ等の公開されたコマンドでアクセスできる、即ち、認証せずに読み書きできる領域である。従って、非認証領域３３１に対しては、フラッシュＡＴＡやコンパクトフラッシュと同じように、ＰＣ１０２上のファイル管理ソフトウェアでデータの読み書きが可能である。

【００３３】３つの記憶領域には、以下の情報を格納することとし、これによって、一般的なＰＣの補助記憶装置として機能と、電子音楽配信に係る音楽データに対する著作権保護の機能とを提供している。つまり、非認証領域３３１には、著作権保護の対象となる音楽データが暗号化された暗号化コンテンツ４２６や、著作権保護とは無関係な一般的なデータであるユーザデータ４２７等が格納される。認証領域３３２には、非認証領域３３１に格納された暗号化コンテンツ４２６を復号するための秘密鍵となる暗号化キー４２５が格納される。そして、特殊領域３０４には、認証領域３３２にアクセスするために必要とされる情報であるメディアＩＤ３４１が格納されている。

【００３４】ＰＣ１０２やプレーヤ２０１は、まず、装着されたメモリカード１０９の特殊領域３０４に格納されたメディアＩＤ３４１を読み出し、それを用いて認証領域３３２に格納された暗号化キー４２５、権利情報を取り出す。それら暗号化キー４２５や権利情報によって再生が許可されていれば、非認証領域３３１にある暗号化コンテンツ４２６を読み出し、暗号化キー４２５で復号しながら、再生を行うことができる。

【００３５】もし、あるユーザが不正に入手した音楽データだけをＰＣ１０２等でメモリカード１０９の非認証領域３３１に書き込み、そのようなメモリカード１０９をプレーヤ２０１に装着して再生しようとしたとする。しかし、そのメモリカード１０９の非認証領域３３１に音楽データが格納されているものの、認証領域３３２に対応する暗号化キー４２５や権利情報が存在しないために、そのプレーヤ２０１は、その音楽データを再生することができない。これによって、正規の暗号化キーや権利情報を伴わないで音楽コンテンツだけをメモリカード１０９に複製しても、その音楽コンテンツは再生されないので、デジタル著作物の不正な複製が防止される。

【００３６】図７は、ＰＣ１０２やプレーヤ２０１がメモリカード１０９の各領域にアクセスする際の制限やコマンドの形態を示す図であり、（ａ）は各領域へのアクセスにおけるルールを示し、（ｂ）は各領域のサイズの変更におけるルールを示し、（ｃ）はメモリカード１０９の領域を示す概念図である。特殊領域３０４は、読み出し専用の領域であり、認証せずに専用コマンドでアクセスできる。この特殊領域３０４に格納されたメディアＩＤ３４１は、認証領域３３２にアクセスするための暗号化コマンドの生成や復号に用いられる。つまり、ＰＣ１０２やプレーヤ２０１は、このメディアＩＤ３４１を読み出し、これを用いて認証領域３３２にアクセスするコマンドを暗号化し、メモリカード１０９に送る。一方、その暗号化コマンドを受けたメモリカード１０９は、メディアＩＤ３４１を用いて、その暗号化コマンドを復号し、解釈して実行する。

【００３７】認証領域３３２は、ＰＣ１０２やプレーヤ２０１等のメモリカード１０９にアクセスする装置とメモリカード１０９との間で認証が成功した時にのみアクセスが可能となる領域であり、その大きさは（ＹＹＹＹ＋１）個のセクタに相当する。つまり、この認証領域３３２は、論理的には、第０～ＹＹＹＹのセクタで構成され、物理的には、フラッシュメモリ３０３の第ＸＸＸＸ～第（ＸＸＸＸ＋ＹＹＹＹ）のセクタアドレスを有するセクタから構成される。なお、セクタアドレスとは、フラッシュメモリ３０３を構成する全てのセクタそれぞれに対してユニークに付された一連の番号のことである。

【００３８】非認証領域３３１は、認証せずにＡＴＡやＳＣＳＩ等の標準コマンドでアクセスすることが可能で、その大きさはＸＸＸＸ個のセクタに相当する。つまり、この非認証領域３３１は、論理的にも物理的にも第０～（ＸＸＸＸ－１）のセクタで構成される。なお、フラッシュメモリ３０３には、認証領域３３２や非認証領

２５）の読み出しに先立ち、認証領域３３２から読み出すためのコマンドを暗号化してメモリカード１０９に送信しておく。

（４）得られた暗号化キー４２５をマスター鍵３２３ａとメディアＩＤ３４１で復号化し、パスワードを抽出する（Ｓ７０５）。このときの復号化は、図８に示されたステップＳ６０５での暗号化の逆変換である。

【００５０】（５）最後に、非認証領域３３１から暗号化コンテンツ４２６を読み出し、上記ステップＳ７０５で抽出したパスワードで復号しながら音楽を再生していく（Ｓ７０６）。このように、メモリカード１０９の非認証領域３３１に格納された音楽データは、認証領域３３２の暗号化キー４２５がないと復号することができない。従って、たとえ不正に音楽データだけを別のメモリカードにコピーしたとしても、その音楽データを正常に再生することができないので、その音楽データの著作権は安全に保護される。

【００５１】また、認証に成功した機器だけがメモリカードの認証領域へのアクセスが許可されるので、認証に用いられるデバイス鍵や暗号化アルゴリズム等を適切に選択して用いることで、一定の条件を満たした機器だけに対してメモリカードの認証領域へのアクセスを許可する等の著作権保護が可能となる。なお、この例では、メモリカード１０９に暗号化コンテンツを記録する際に、その暗号化に用いられたパスワードをマスター鍵とメディアＩＤで暗号化し、暗号化キーとして認証領域３３２に格納されたが（Ｓ６０５）、マスター鍵及びメディアＩＤのいずれかを用いて暗号化することとしてもよい。これによって、暗号の強度が低下する恐れがあるものの、暗号化の簡略化に伴い、メモリカード１０９やプレーヤ２０１等の回路規模が小さくなるという利点が得られる。

【００５２】また、プレーヤ２０１やＰＣ１０２は、認証により、メモリカード１０９からマスター鍵３２３ａを取り出したが、予めプレーヤ２０１やＰＣ１０２にそのマスター鍵３２３ａを埋め込んでおいてもよいし、マスター鍵３２３ａを暗号化し、暗号化マスター鍵として特殊領域３０４に格納しておいてもよい。次に、このようなメモリカードの認証領域の活用例として、「読み出し回数」を格納した例と、「デジタル出力許可回数」を格納した例を示す。

【００５３】図１０は、プレーヤ２０１（及びＰＣ１０２）がメモリカード１０９の認証領域に格納された読み出し回数８１２を操作する動作を示すフロー図である。ここでは、メモリカード１０９に格納された読み出し回数８１２の範囲内でのみ、プレーヤ２０１が、メモリカード１０９の非認証領域３３１に格納された音楽データを音声信号に再生することが許可されている場合（Ｓ８０１）について説明する。

【００５４】（１）プレーヤ２０１は、デバイス鍵２１ａ等を用いて、メモリカード１０９の認証部３２１とチャレンジ・レスポンス型の認証を行い、その認証に成功すると、まず、メモリカード１０９からマスター鍵３２３ａを取り出す（Ｓ８０２）。

（２）次に、専用コマンドを用いて、メモリカード１０９の特殊領域３０４に格納されているメディアＩＤ３４１を取り出す（Ｓ８０３）。

【００５５】（３）続いて、メモリカード１０９の認証領域３３２から音楽データの暗号化キー４２５を取り出す（Ｓ７０４）。このときには、データ（暗号化キー４２５）の読み出しに先立ち、認証領域３３２から読み出すためのコマンドを暗号化してメモリカード１０９に送信しておく。

（４）次に、メモリカード１０９の認証領域３３２から読み出し回数８１２を取り出し、その値を検査する（Ｓ８０４）。その結果、その値が無制限な読み出しを許可する旨の値である場合は、図９に示された手順（Ｓ７０４～Ｓ７０６）と同様の手順に従って、音楽を再生する（Ｓ８０６～Ｓ８０８）。

【００５６】（５）一方、読み出し回数８１２が０を示す場合は、もはや再生が許可されていないと判定し（Ｓ８０５）、再生処理を終了する（Ｓ８０９）。そうでない場合は、その読み出し回数８１２を１つ減算し、その結果を認証領域３３２に書き戻した後に（Ｓ８０５）、上記手順に従って、音楽を再生する（Ｓ８０６～Ｓ８０８）。

【００５７】このように、メモリカード１０９の認証領域３３２に、予め許可された再生回数を指定した読み出し回数８１２を格納しておくことにより、プレーヤ２０１による音楽再生の回数をコントロールすることが可能となる。これによって、例えば、レンタルＣＤやＫＩＯＳＫ端末等によるアナログ再生に適用することが可能となる。

【００５８】なお、読み出し回数８１２に代えて、「読み出し時間」とすることで、音楽コンテンツを再生することが可能な総時間を制限することもできる。また、回数と時間とを組み合わせてもよい。さらに、読み出し回数８１２は、再生を開始してから１０秒等の一定時間を超えて再生され続けた場合にだけ、その回数を減算してもよい。また、読み出し回数８１２は、不正な改ざんを防ぐために暗号化して格納することとしてもよい。

【００５９】図１１は、プレーヤ２０１（及びＰＣ１０２）がメモリカード１０９の認証領域に格納されたデジタル出力許可回数９１３を操作する動作を示すフロー図である。ここでは、メモリカード１０９に格納されたデジタル出力許可回数９１３の範囲内でのみ、プレーヤ２０１が、メモリカード１０９の非認証領域３３１に格納された音楽データを読み出してデジタル出力することが許可されている場合（Ｓ９０１）について説明する。

【００６０】（１）プレーヤ２０１は、図９に示された

ンター値としてＰＣ１０２等に送る（Ｓ１００２）。

【００７０】（２）取得したカウンター値と、既に取得しているマスター鍵３２３ａ及びメディアＩＤ３４１とからパスワードを生成する（Ｓ１００３）。

（３）書き込むべき１セクタ分のデータをパスワードで暗号化しながら、メモリカード１０９に送る（Ｓ１００４）。このとき、書き込むべきセクタを指定する情報や、暗号化に用いたカウンター値も一緒に送る

（４）メモリカード１０９は、受け取った暗号化データを、指定されたセクタ１００４に書き込む（Ｓ１００６）。

【００７１】（５）その暗号化データからＥＣＣを計算し、上記セクタに対応する拡張領域１００５に、ＥＣＣデータ１００６として書き込む（Ｓ１００７）。

（６）続いて、上記暗号化データとともに受け取ったカウンター値を時変領域１００７に書き込む（Ｓ１００８）。次に、ＰＣ１０２がメモリカード１０９からデータを読み出す場合（Ｓ１０１１）の手順を説明する。

【００７２】（１）ＰＣ１０２は、メモリカード１０９に対して、セクタを指定するとともにデータの読み出しを要求する。すると、メモリカード１０９は、まず、指定されたセクタ１００４の暗号化データだけを読み出してＰＣ１０２に出力し（Ｓ１０１６）、ＰＣ１０２は、その暗号化データを受け取る（Ｓ１０１２）。

（２）次に、メモリカード１０９は、指定されたセクタ１００４に対応する拡張領域１００５の時変領域１００７に格納されたカウンター値を読み出してＰＣ１０２に出力し（Ｓ１０１７）、ＰＣ１０２は、そのカウンター値を受け取る（Ｓ１０１３）。

【００７３】（３）読み出したカウンター値と、既に取得しているマスター鍵３２３ａ及びメディアＩＤ３４１とからパスワードを生成する（Ｓ１０１４）。

（４）そのパスワードを用いて、暗号化データを復号する（Ｓ１０１５）。ここで、もし、不正な改ざん等により、セクタ１００４のデータが変更されている場合には、時変領域１００７から読み出されたカウンター値との不整合が生じ、元のデータに復元されない。

【００７４】このように、フラッシュメモリ３０３内に、ユーザからは見えない（アクセスできない）隠し領域としての時変領域１００７を設け、そこに格納されたカウンター値に依存したパスワードでデータを暗号化し格納することで、不正なユーザによるデータの改ざんを防止することができる。なお、ここでは、時変領域１００７は、ＥＣＣを格納するための拡張領域１００５としたが、メモリカードの外部から書き換えができない領域であれば、フラッシュメモリ３０３内の他の領域に設けてもよい。

【００７５】また、カウンター値は、乱数であったが、刻々と変化する時刻等のタイマー値としたり、フラッシュメモリ３０３への書き込み回数を示す値としてもよい。次に、フラッシュメモリ３０３の論理アドレスと物理アドレスとの対応づけについて、好ましい例を説明する。図１３は、論理アドレスと物理アドレスとの対応を変更する様子を示す図であり、（ａ）は変更前の対応関係、（ｂ）は変更後の対応関係、（ｃ）は（ａ）に対応する変換テーブル１１０１、（ｄ）は（ｂ）に対応する変換テーブル１１０１を示す。

【００７６】ここで、変換テーブル１１０１は、全ての論理アドレス（ここでは、論理ブロックの番号）と各論理アドレスに対応する物理アドレス（ここでは、フラッシュメモリ３０３を構成する物理ブロックの番号）とを組にして記憶するテーブルであり、コントロールＩＣ３０２内の不揮発な記憶領域等に保存され、認証領域アクセス制御部３２５や非認証領域アクセス制御部３２６によって論理アドレスを物理アドレスに変換する際等において参照される。

【００７７】メモリカード１０９にアクセスする機器は、メモリカード１０９中の物理的に存在するすべてのデータ空間（フラッシュメモリ３０３を構成する全ての物理ブロック）にデータを書き込めるのではなく、論理アドレスによって特定できる論理的なデータ空間（論理ブロック）にのみデータを書き込むことができる。この理由の一つは、フラッシュメモリ３０３の一部が破損し読み書きが行えなくなった場合に、その領域を置き換えるための代替領域を確保しておかなければならないからである。そして、そのような欠陥ブロックを代替領域中のブロックと置き換えた場合であっても、その対応づけの変更を変換テーブルに反映しておくことで、複数の連続する物理ブロックからなるファイルの論理的な連続性は維持されるので、外部機器に対しては破損が生じなかったように見せかけることができる。

【００７８】ところが、複数のブロックからなるファイル等をメモリカード１０９に格納したり、削除したりすることを繰り返していると、論理ブロックのフラグメンテーションが増大する。つまり、図１３（ａ）に示されるように、同一のファイルfilelを構成する論理ブロックであるにも拘わらず、それらの論理アドレスが不連続となってしまう。

【００７９】これでは、例えば、音楽データをメモリカード１０９に格納しようとしたときに、メモリカード１０９の論理的な連続領域に書けないので、各ブロック毎に書き込みコマンド「Write address count」を発行する必要があり、書き込み速度が低下してしまう。同様に、読み出し動作においても、１曲を構成する音楽データであるにも拘わらず、各ブロック毎に読み出しコマンド「Read address count」を発行する必要があり、音楽データのリアルタイム再生が困難となってしまう。

【００８０】この問題を解決する方法として、このメモリカード１０９のコントロールＩＣ３０２は、外部機器からのコマンドに基づいて、変換テーブル１１０１を書

ブロック（ここでは、物理ブロック４と５）を特定した後に（ステップＳ１２０３）、メモリカード１０９に対して、それらブロック４と５の番号を指定した消去コマンドを発行する（ステップＳ１２０４）。そのコマンドを受信したメモリカード１０９のコマンド判定制御部３２２は、アクセス制御部３２５、３２６に指示を出す等により、指定された物理ブロック４と５を一括消去する。

【００９１】これによって、もし、その物理ブロック４と５への書き込みが発生した場合には、その物理ブロックに対する消去処理は不要となるので、高速な書き込みが可能となる。次に、このメモリカード１０９が有する個人データの保護に関する機能、具体的には、メモリカード１０９が外部機器を認証する際にその外部機器を使用するユーザの個人データを必要とする場合における個人データの保護機能について説明する。ここで、個人データとは、そのユーザを一意に識別するためのデータであって、メモリカード１０９の認証領域３３２へのアクセスが許可された正規のユーザとしてメモリカード１０９に識別させるためのデータである。

【００９２】このような場合において、認証領域３３２へのアクセスの度にユーザに対して繰り返し個人データを入力することを要求したり、その個人データを認証領域３３２に格納することとしたのでは、不正者によって盗聴されたり、認証領域３３２にアクセスする権限を有する他のユーザによって見られたりする不都合がある。

【００９３】これを防止するために、音楽データと同様に、個人データについても、個人が設定したパスワードで暗号化してから格納するという方法が考えられる。しかしながら、パスワードを設定した場合には、その個人データを見るたびにパスワードを入力しなければならず、手続が面倒であり、その管理も必要となる。そこで、このメモリカード１０９は、不必要に個人データを繰り返し入力することを回避する機能を有する。

【００９４】図１５は、認証のためのプレーヤ２０１とメモリカード１０９間の通信シーケンス及び主要な構成要素を示す図である。なお、本図に示される処理は、主にプレーヤ２０１の認証回路２１６及びメモリカード１０９の認証部３２１によって実現される。本図に示されるように、プレーヤ２０１の認証回路２１６は、暗号化及び復号化等の機能の他に、メモリカード１０９に保持されたマスター鍵３２３ａと同一の秘密鍵であるマスター鍵１３０１と、製造番号（ｓ／ｎ）等のプレーヤ２０１に固有のＩＤである機器固有ＩＤ１３０２とを予め記憶している。

【００９５】また、メモリカード１０９の認証部３２１は、暗号化、復号化及び比較等の機能に他に、２つの不揮発な記憶領域である機器固有ＩＤ群記憶領域１３１０とユーザキー記憶領域１３１１とを有する。機器固有ＩＤ群記憶領域１３１０は、このメモリカード１０９の認証領域３３２へのアクセスが許可された全ての機器の機器固有ＩＤを記憶しておくための記憶領域であり、ユーザキー記憶領域１３１１は、個人データとして機器から送られてきたユーザキーを記憶しておくための記憶領域である。

【００９６】具体的な認証手順は、以下の通りである。なお、送受信においては、全てのデータは暗号化されて送信され、受信側で復号される。そして、手順が進む度に、次の手順での暗号化及び復号化に用いられる鍵が生成される。

（１）メモリカード１０９とプレーヤ２０１とを接続すると、まず、プレーヤ２０１は、マスター鍵１３０１を用いて機器固有ＩＤ１３０２を暗号化し、メモリカード１０９に送る。

【００９７】（２）メモリカード１０９は、受け取った暗号化された機器固有ＩＤ１３０２をマスター鍵３２３ａで復号し、得られた機器固有ＩＤ１３０２が既に機器固有ＩＤ群記憶領域１３１０に格納されているか検査する。

（３）その結果、既に機器固有ＩＤ１３０２が格納されている場合は、認証が成功した旨をプレーヤ２０１に通知し、一方、機器固有ＩＤ１３０２が格納されていない場合は、プレーヤ２０１に対しユーザキーを要求する。

【００９８】（４）プレーヤ２０１は、ユーザキーの入力をユーザに促した後に、ユーザから個人データとしてのユーザキーを取得し、そのユーザキーをメモリカード１０９に送る。

（５）メモリカード１０９は、送られてきたユーザキーと予めユーザキー記憶領域１３１１に格納されているものとを比較し、一致している場合、又は、ユーザキー記憶領域１３１１が空であった場合は、認証が成功した旨をプレーヤ２０１に通知するとともに、上記ステップ（３）で獲得した機器固有ＩＤ１３０２を機器固有ＩＤ群記憶領域１３１０へ格納する。

【００９９】これによって、ユーザが所有する機器とメモリカード１０９とを初めて接続した場合は個人データ（ユーザキー）の入力が必要とされるが、２回目以降においては、その機器の機器固有ＩＤが用いられて自動的に認証が成功するので、再び、個人データの入力を要求されることはない。次に、本メモリカード１０９とＰＣ１０２やプレーヤ２０１等の外部機器との認証プロトコルの変形例について、図１６及び図１７を用いて説明する。

【０１００】図１６は、変形例に係るメモリカード１０９と外部機器（ここでは、プレーヤ２０１）との認証手順を示す通信シーケンス図である。ここでの処理は、主に、変形例に係るプレーヤ２０１の認証回路２１６、ＰＣ１０２の制御プログラム１１１ｂ及びメモリカード１０９の認証部３２１によって実現される。また、メモリカード１０９のマスター鍵記憶部３２３には、暗号化さ

ンスデータと、チャレンジデータとして送った乱数を暗号化して得られる暗号化チャレンジデータとを比較し、一致している場合には、メモリカード１０９の認証に成功した（ＯＫ）と認識し、そのメモリカード１０９の認証領域３３２へのアクセスコを行う。一方、比較の結果、一致しなかった場合には、認証に成功しなかった（ＮＧ）したと認識し、そのメモリカード１０９の認証領域３３２へのアクセスは断念する。

【０１１０】なお、これら相互認証における暗号化アルゴリズムは、メモリカード１０９及びプレーヤ２０１が正当な機器である限り、全て同一である。また、メモリカード１０９及びプレーヤ２０１は、それぞれの認証及び証明において生成した暗号化チャレンジデータとレスポンスデータとを排他的論理和演算し、得られた結果をセキュア鍵として、メモリカード１０９の認証領域３３２へのアクセスのために用いる。そうすることで、双方の機器１０９及び２０１が相互認証に成功した場合にのみ共通となり、かつ、時変のセキュア鍵を共有し合うことが可能となり、これによって、認証領域３３２にアクセスする条件として相互認証に成功していることが条件とされることになる。

【０１１１】なお、セキュア鍵の生成方法として、暗号化チャレンジデータとレスポンスデータとセキュアメディアＩＤとの排他的論理和をとることとしてもよい。次に、本メモリカード１０９の認証領域３３２と非認証領域３３１との境界線の変更機能についての変形例について、図１８及び図１９を用いて説明する。図１８は、境界線を変更する前のフラッシュメモリ３０３の使用状態を示す図である。図１８（ａ）は、フラッシュメモリ３０３の物理ブロックの構成を示すメモリマップである。

【０１１２】図１８（ｂ）は、非認証領域アクセス制御部３２６内の不揮発な記憶領域等に置かれる非認証領域３３１専用の変換テーブル１１０３であり、非認証領域３３１の論理ブロックと物理ブロックとの対応関係が格納されている。非認証領域アクセス制御部３２６は、この変換テーブル１１０３を参照することで、論理アドレスを物理アドレスに変換したり、割り当て領域を越えるアクセス違反を検出することができる。

【０１１３】図１８（ｃ）は、認証領域アクセス制御部３２５内の不揮発な記憶領域等に置かれる認証領域３３２専用の変換テーブル１１０２であり、認証領域３３２の論理ブロックと物理ブロックとの対応関係が格納されている。認証領域アクセス制御部３２５は、この変換テーブル１１０２を参照することで、論理アドレスを物理アドレスに変換したり、割り当て領域を越えるアクセス違反を検出することができる。

【０１１４】境界線の変更前においては、図１８（ａ）に示されるように、フラッシュメモリ３０３の代替領域を除いた記憶領域（物理ブロック００００～ＥＦＦＦ）のうち、境界線よりも下位アドレスに位置する物理ブロック０００～ＤＦＦＦが非認証領域３３１に割り当てられ、上位アドレスに位置する物理ブロックＥ０００～ＥＦＦＦが認証領域３３２に割り当てられている。

【０１１５】そして、図１８（ｂ）に示された変換テーブル１１０２から分かるように、非認証領域３３１においては、物理ブロックと論理ブロックの番号が一致するように対応づけられている。一方、図１８（ｃ）に示された変換テーブル１１０３から分かるように、認証領域３３２においては、物理ブロックと論理ブロックとは、その番号の並びが逆順になっている。つまり、論理ブロック０００～０ＦＦＦそれぞれが物理ブロックＥＦＦＦ～Ｅ０００に対応している。これは、論理ブロックは昇順に使用されていくことと、境界線が移動された場合において領域変更の生じた物理ブロックのデータ退避や移動処理の手間を考慮したからである。

【０１１６】図１９（ａ）～（ｃ）は、境界線を変更した後のフラッシュメモリ３０３の使用状態を示す図であり、それぞれ、変更前の図１８（ａ）～（ｃ）に対応する。なお、境界線の変更は、そのアドレスを指定する専用のコマンドがコマンドピンからコマンド判定制御部３２２に入力されたときに、コマンド判定制御部３２２によって認証領域アクセス制御部３２５内の変換テーブル１１０２及び非認証領域３３１内の変換テーブル１１０３が書き換えられることにより、実現される。

【０１１７】図１９（ａ）～（ｃ）に示されるように、ここでは、物理ブロックＥ０００とＤＦＦＦ間に置かれていた境界線が物理ブロックＤ０００とＣＦＦＦ間に移動されている。つまり、非認証領域３３１のサイズを１０００（hex）個だけ減少させ、認証領域３３２のサイズを１０００（hex）だけ増加させている。それに伴って、図１９（ｂ）に示されるように、非認証領域３３１の変換テーブル１１０３のサイズは、１０００（hex）個のエントリー分だけ減少され、その結果、論理ブロック０００～ＣＦＦＦに対応する物理ブロック０００～ＣＦＦＦが示されている。一方、図１９（ｃ）に示されるように、認証領域３３２の変換テーブル１１０２のサイズは、１０００（hex）個のエントリー分だけ増加され、その結果、論理ブロック０００～１ＦＦＦに対応する物理ブロックＥＦＦＦ～Ｄ０００が示されている。

【０１１８】このように、フラッシュメモリ３０３の一定領域において境界線によって非認証領域と認証領域とを区切り、その境界線の移動によって各領域のサイズを変更することにより、このメモリカード１０９の多様な応用、例えば、保護すべきデジタル著作物の格納を主要な用途とする場合やその逆の場合等に対応させることが可能となる。

【０１１９】そして、非認証領域及び認証領域いずれにおいても、境界線に遠いアドレスの物理ブロックから境界線に近いアドレスの物理ブロックに向かって、使用し

ズ変更回路は、前記一定サイズの記憶領域を２分する境界アドレスを変更することによって前記認証領域及び前記非認証領域それぞれの領域サイズを変更するとしてもよい。これによって、境界線を移動させるだけで認証領域及び非認証領域の領域サイズを変更することができるので、そのための回路は小さくて済む。

【０１３０】また、前記領域サイズ変更回路は、前記認証領域における論理アドレスと物理アドレスとの対応を示す認証領域変換テーブルと、前記非認証領域における論理アドレスと物理アドレスとの対応を示す非認証領域変換テーブルと、前記電子機器からの命令に従って前記認証領域変換テーブル及び前記認証領域変換テーブルを変更する変換テーブル変更部とを有し、前記認証領域アクセス制御部は、前記認証領域変換テーブルに基づいて前記電子機器によるアクセスを制御し、前記非認証領域アクセス制御部は、前記非認証領域変換テーブルに基づいて前記電子機器によるアクセスを制御するとしてもよい。

【０１３１】これによって、認証領域と非認証領域で、変換テーブルが独立分離されているので、それぞれの領域サイズや論理アドレスと物理アドレスとの対応を個別に管理することが容易となる。また、前記認証領域及び前記非認証領域は、それぞれ、前記一定サイズの記憶領域を２分して得られる物理アドレスの高い領域及び低い領域に割り当てられ、前記非認証領域変換テーブルは、論理アドレスの昇順が物理アドレスの昇順となるように論理アドレスと物理アドレスとが対応づけられ、前記認証領域変換テーブルは、論理アドレスの昇順が物理アドレスの降順となるように論理アドレスと物理アドレスとが対応づけられているとしてもよい。

【０１３２】これによって、論理アドレスの昇順に使用していくことで、認証領域と非認証領域との境界付近の領域が使用される確立が低くなるので、その境界を移動させた場合に必要とされるデータ退避や移動等の処理が発生する確率も低くなり、領域サイズの変更が簡単化される。また、前記半導体メモリカードはさらに、予めデータが格納された読み出し専用のメモリ回路を備えてもよい。これによって、他の半導体メモリカードと区別できる識別データ等を読み出し専用メモリに格納し、デジタル著作物をその識別データに依存させて格納したりすることで、著作権保護の機能が強化される。

【０１３３】また、前記認証領域及び前記非認証領域は、前記電子機器にとって読み書き可能な記憶領域と読み出し専用の記憶領域とからなり、前記制御回路はさらに、前記電子機器が前記不揮発メモリにデータを書き込むためのアクセスをする度に乱数を発生する乱数発生器を有し、前記認証領域アクセス制御部及び前記非認証領域アクセス制御部は、前記乱数を用いて前記データを暗号化し、得られた暗号化データを前記読み書き可能な記憶領域に書き込むとともに、前記乱数を前記暗号化データに対応づけられた前記読み出し専用の記憶領域に書き込むとしてもよい。

【０１３４】これによって、読み書き可能な記憶領域に対する不正な改ざん等が行われても、読み出し専用の記憶領域に格納された乱数との整合性を検査することで、そのような行為を検出することが可能となるので、より安全なデータ記録が実現される。また、前記制御回路はさらに、前記認証領域及び前記非認証領域における論理アドレスと物理アドレスとの対応を示す変換テーブルと、前記電子機器からの命令に従って前記変換テーブルを変更する変換テーブル変更部とを有し、前記認証領域アクセス制御部及び前記非認証領域アクセス制御部は、前記変換テーブルに基づいて前記電子機器によるアクセスを制御するとしてもよい。

【０１３５】これによって、同一ファイルを構成する複数の論理ブロックが断片化する現象が生じても、論理的に連続した論理ブロックとなるように容易に変更することができるので、同一ファイルへのアクセスが高速化される。また、前記制御回路はさらに、前記認証領域及び前記非認証領域に書き込むべきデータを暗号化するとともに、前記認証領域及び前記非認証領域から読み出されたデータを復号化する暗号復号部を有してもよい。これによって、半導体メモリカードを破壊して認証領域及び非認証領域のメモリ内容を直接読み出す等の不正な攻撃に耐えることが可能となる。

【０１３６】また、前記不揮発メモリは、フラッシュメモリであり、前記制御回路はさらに、前記電子機器からの命令に従って、前記認証領域及び前記認証領域に存在する未消去の領域を特定し、その領域を示す情報を前記電子機器に送る未消去リスト読み出し部を有してもよい。これによって、電子機器は、フラッシュメモリの書き換えに先立って、未消去の領域を知り、その領域を事前に消去しておくことができるので、高速な書き換えが可能となる。

【０１３７】また、前記認証部は、認証のために電子機器を使用するユーザに対してそのユーザに固有の情報であるユーザキーを要求するものであり、前記制御回路はさらに、前記ユーザキーを記憶しておくためのユーザキー記憶部と、前記認証部による認証に成功した電子機器を特定することができる識別情報を記憶しておくための識別情報記憶部と、前記認証部による認証が開始されると、その電子機器から識別情報を取得し、その識別情報が前記識別情報記憶部に既に格納されているか否か検査し、既に格納されている場合には、前記認証部によるユーザキーの要求を禁止させるユーザキー要求禁止部とを有してもよい。

【０１３８】これによって、半導体メモリカードと接続して使用する度にパスワードや個人データの入力が要求されるという手間が回避されるので、不正に個人データが盗聴されて利用されるという不具合の発生が抑えられ

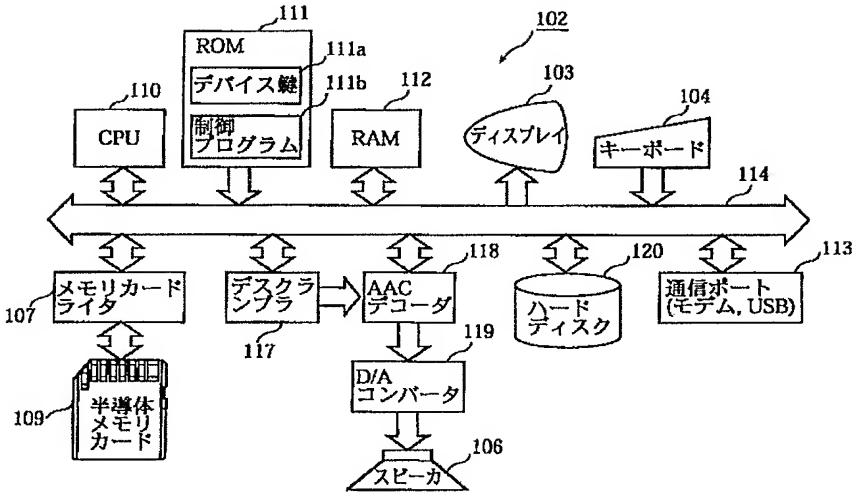
換テーブルを示し、（ｃ）は認証領域専用の変換テーブルを示す。

【図１９】同半導体メモリカードの認証領域と非認証領域との境界線の変更における変更後の状態を示す図であり、（ａ）はフラッシュメモリの物理ブロックの構成を示すメモリマップであり、（ｂ）は非認証領域専用の変換テーブルを示し、（ｃ）は認証領域専用の変換テーブルを示す。

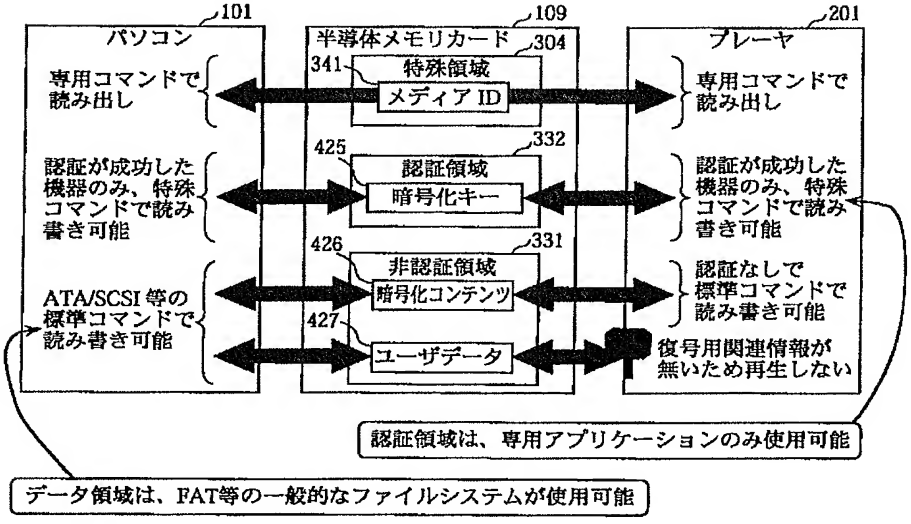
【符号の説明】

１０１　通信回線
１０２　ＰＣ
１０３　ディスプレイ
１０４　キーボード
１０５　メモリカードライタ挿入口
１０６　スピーカ
１０７　メモリカードライタ
１０８　メモリカード挿入口
１０９　メモリカード
１１０　ＣＰＵ
１１１　ＲＯＭ
１１２　ＲＡＭ
１１３　通信ポート
１１４　内部バス
１１７　デスクランブラ
１１８　ＡＡＣデコーダ
１１９　Ｄ／Ａコンバータ
１２０　ハードディスク
２０１　プレーヤ
２０２　操作ボタン
２０３　液晶表示部
２０４　アナログ出力端子
２０５　デジタル出力端子
２０６　メモリカード挿入口
２０８　ヘッドフォン
２１０　ＣＰＵ
２１１　ＲＯＭ
２１２　ＲＡＭ
２１３　通信ポート
２１４　内部バス
２１５　カードＩ／Ｆ部
２１６　認証回路
２１７　デスクランブラ
２１８　ＡＡＣデコーダ
２１９　Ｄ／Ａコンバータ
２２０　ＡＡＣエンコーダ
２２１　Ａ／Ｄコンバータ
２２２　スクランブラ
２２３　アナログ入力端子
２２４　スピーカ
３０２　コントロールＩＣ
３０３　フラッシュメモリ
３０４　ＲＯＭ（特殊領域）
３２１　認証部
３２２　コマンド判定制御部
３２３　マスター鍵記憶部
３２３ａ　マスター鍵
３２３ｂ　暗号化マスター鍵
３２４　特殊領域アクセス制御部
３２５　認証領域アクセス制御部
３２６　非認証領域アクセス制御部
３２７　暗号・復号化回路
３３１　非認証領域
３３２　認証領域
３４１　メディアＩＤ
３４２　製造メーカ名
３４３　セキュアメディアＩＤ
４２５　暗号化キー
４２６　暗号化コンテンツ
４２７　ユーザデータ
５０１　代替ブロック領域
８１２　読み出し回数
９１３　デジタル出力許可回数
１００３　乱数発生器
１００４　セクタ
１００５　拡張領域
１００６　ＥＣＣデータ
１００７　時変領域
１１０１　変換テーブル
１１０２　認証領域専用変換テーブル
１１０３　非認証領域専用変換テーブル
１２０３　未消去リスト
１３０１　マスター鍵
１３０２　機器固有ＩＤ
１３１０　機器固有ＩＤ群記憶領域
１３１１　ユーザキー記憶領域

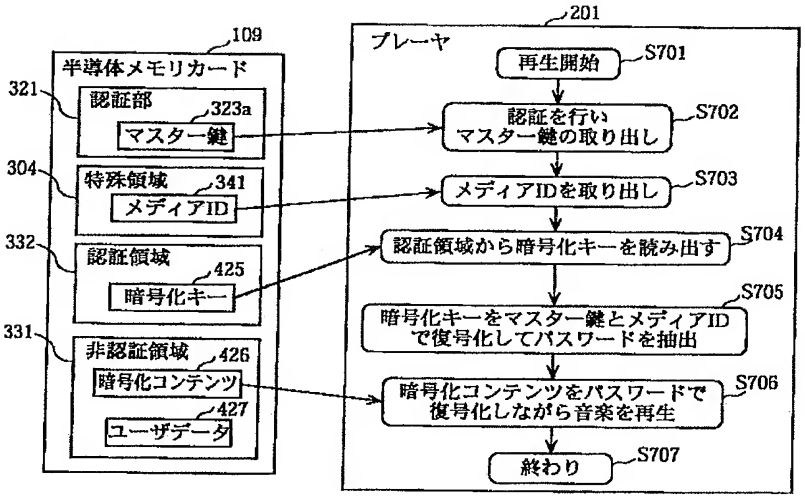
【図３】


111
ROM
111a
デバイス鍵
111b
制御プログラム
112
RAM
110
CPU
102
103
ディスプレイ
104
キーボード
114
メモリカードライタ
107
デスクランブラ
117
AACデコーダ
118
ハードディスク
120
通信ポート(モデム, USB)
113
119
D/Aコンバータ
106
スピーカ
109
半導体メモリカード

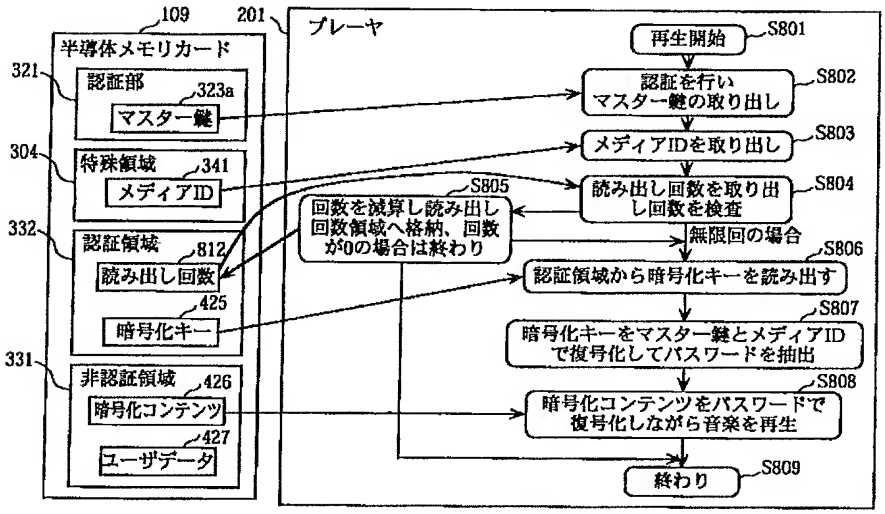
【図６】


101
パソコン
109
半導体メモリカード
304
201
プレーヤ
専用コマンドで読み出し
341
特殊領域
メディアID
専用コマンドで読み出し
認証が成功した機器のみ、特殊コマンドで読み書き可能
425
認証領域
暗号化キー
332
認証が成功した機器のみ、特殊コマンドで読み書き可能
426
非認証領域
暗号化コンテンツ
331
ATA/SCSI等の標準コマンドで読み書き可能
認証なしで標準コマンドで読み書き可能
427
ユーザデータ
復号用関連情報が無いため再生しない
認証領域は、専用アプリケーションのみ使用可能
データ領域は、FAT等の一般的なファイルシステムが使用可能

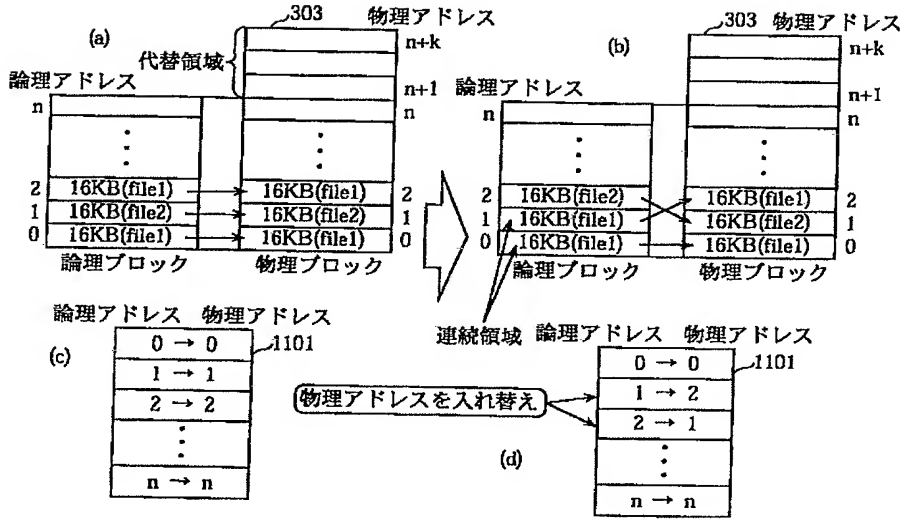
【図９】


109
半導体メモリカード
321
認証部
323a
マスター鍵
304
特殊領域
341
メディアID
332
認証領域
425
暗号化キー
331
非認証領域
426
暗号化コンテンツ
427
ユーザデータ
201
プレーヤ
再生開始
S701
認証を行い
マスター鍵の取り出し
S702
メディアIDを取り出し
S703
認証領域から暗号化キーを読み出す
S704
暗号化キーをマスター鍵とメディアID
で復号化してパスワードを抽出
S705
暗号化コンテンツをパスワードで
復号化しながら音楽を再生
S706
終わり
S707

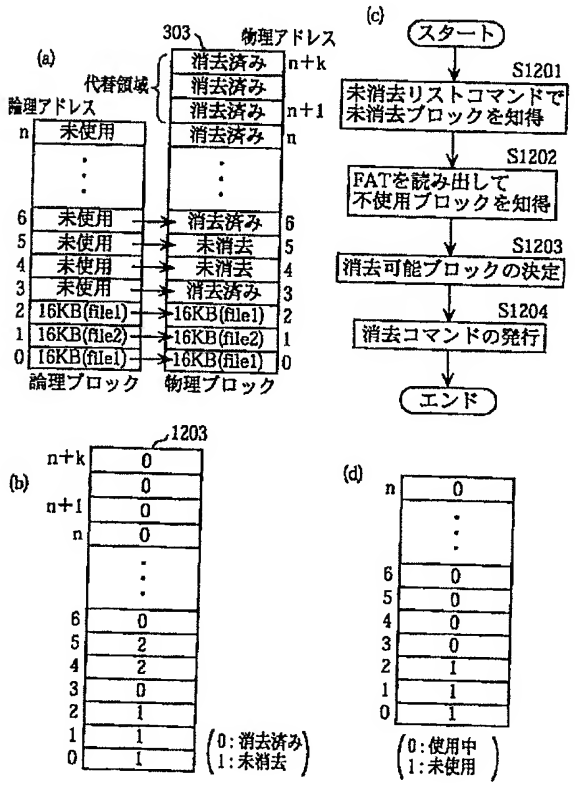
【図１０】


109
201
半導体メモリカード
321
認証部
323a
マスター鍵
304
特殊領域
341
メディアID
332
認証領域
812
読み出し回数
425
暗号化キー
331
非認証領域
426
暗号化コンテンツ
427
ユーザデータ
プレーヤ
再生開始
S801
認証を行い
マスター鍵の取り出し
S802
メディアIDを取り出し
S803
読み出し回数を取り出
し回数を検査
S804
S805
回数を減算し読み出し
回数領域へ格納、回数
が0の場合は終わり
無限回の場合
S806
認証領域から暗号化キーを読み出す
S807
暗号化キーをマスター鍵とメディアID
で復号化してパスワードを抽出
S808
暗号化コンテンツをパスワードで
復号化しながら音楽を再生
終わり
S809

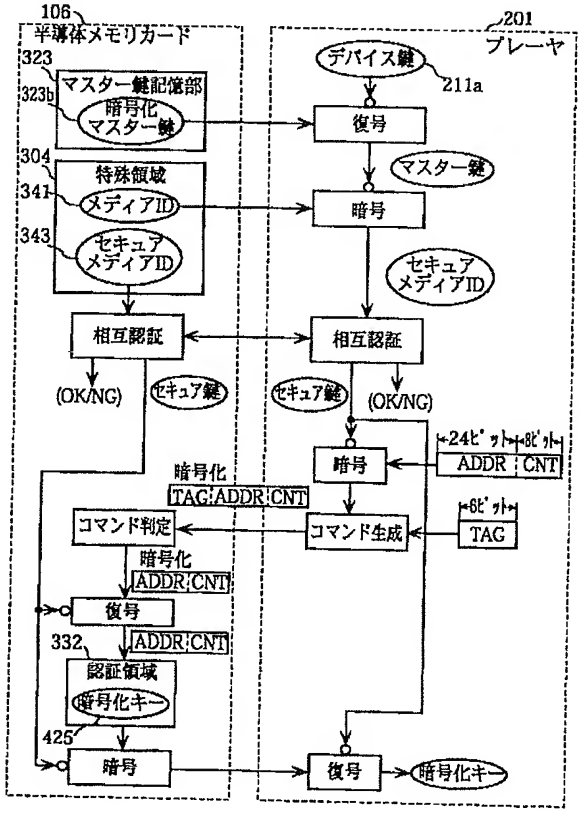
【図１３】


(a)
303 物理アドレス
代替領域
論理アドレス
n+k
n+1
n
2 16KB(file1)
1 16KB(file2)
0 16KB(file1)
論理ブロック
物理ブロック
(b)
303 物理アドレス
論理アドレス
2 16KB(file2)
1 16KB(file1)
0 16KB(file1)
16KB(file1) 2
16KB(file2) 1
16KB(file1) 0
連続領域
(c)
論理アドレス 物理アドレス
0 → 0
1 → 1
2 → 2
n → n
1101
物理アドレスを入れ替え
(d)
論理アドレス 物理アドレス
0 → 0
1 → 2
2 → 1
n → n
1101

【図１４】


(a)
303 物理アドレス
代替領域
論理アドレス
消去済み
未使用
6 未使用 → 消去済み
5 未使用 → 未消去
4 未使用 → 未消去
3 未使用 → 消去済み
2 16KB(file1) → 16KB(file1)
1 16KB(file2) → 16KB(file2)
0 16KB(file1) → 16KB(file1)
論理ブロック
物理ブロック
(b)
1203
0:消去済み
1:未消去
(c)
スタート
S1201
未消去リストコマンドで
未消去ブロックを知得
S1202
FATを読み出して
不使用ブロックを知得
S1203
消去可能ブロックの決定
S1204
消去コマンドの発行
エンド
(d)
0:使用中
1:未使用

【図１６】


106
半導体メモリカード
323
マスター鍵記憶部
323b
暗号化
マスター鍵
304
特殊領域
341
メディアID
343
セキュア
メディアID
相互認証
(OK/NG)
セキュア鍵
暗号化
TAG ADDR CNT
コマンド判定
暗号化
ADDR CNT
復号
332
認証領域
暗号化キー
425
暗号
201
プレーヤ
デバイス鍵
211a
復号
マスター鍵
暗号
セキュア
メディアID
相互認証
セキュア鍵
(OK/NG)
24ビット
8ビット
暗号
ADDR CNT
コマンド生成
TAG
復号
暗号化キー

Ｆターム(参考) 5B017 AA07 BA05 BA07 BB02 BB10
CA14
5B035 AA06 AA13 BB09 BC00 CA07
CA11 CA38
5B058 CA25 CA27 KA02 KA06 KA35
YA16
5J104 AA07 KA02 NA02 NA05 NA33
NA35 NA41 PA14